Received April 16, 2019, accepted April 29, 2019, date of publication May 3, 2019, date of current version May 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2914722

Color Image Compression-Encryption Algorithm Based on Fractional-Order Memristor Chaotic Circuit

FEIFEI YANG[1], JUN MOU[1], KEHUI SUN[2], YINGHONG CAO[1], AND JIYU JIN[1]

[1]School of Information Science and Engineering, Dalian Polytechnic University, Dalian 116034, China
[2]School of Physics and Electronics, Central South University, Changsha 410083, China

Corresponding author: Jun Mou (moujun@csu.edu.cn)

This work was supported in part by the Basic Scientific Research Projects of Colleges and Universities of Liaoning Province under Grant 2017J045, in part by the Provincial Natural Science Foundation of Liaoning under Grant 20170540060, in part by the Scientific Research Projects in General of Liaoning Province under GrantL2015043, and in part by the Doctoral Research Startup Fund Guidance Program of Liaoning Province under Grant 201601280.

ABSTRACT In this paper, a fractional-order memristive chaotic circuit system is defined according to memristor circuit. The dynamic characteristics are analyzed through the phase diagram, bifurcation diagram, and Lyapunov exponent spectrum, and the randomness of the chaotic pseudo-random sequence is tested by NIST SP800-22. Based on this fractional-order memristive chaotic circuit, we propose a novel color image compression-encryption algorithm. In this algorithm, compression sensing (CS) algorithm is used for compression image, and then using Zigzag confusion, add modulus and BitCircShift diffuse encrypt the image. The theoretical analysis and simulation results indicate that the proposed compression and encryption scheme has good compression performance, reconstruction effect, and higher safety performance. Moreover, it also shows that the new algorithm facilitates encryption, storage, and transmission of image information in practical applications.

INDEX TERMS Color image encryption, compression sensing (CS), zigzag confusion, add modulus and BitCircShift diffuse, fractional-order memristive chaotic circuit.

I. INTRODUCTION

As the development of science and technology, the information safety becomes important. Compared with other information carriers, color image has more information. Therefore, it is necessary for us to study color image encryption.

Due to the inherent performance of chaotic system with randomness, non-periodicity and sensitivity to parameters and initial values [1]– [3], it is widely applied to image encryption algorithm. At the moment, various color image encryption algorithms using chaotic system were proposed [4]– [21]. Huang *et al.* applied the unpredictable characteristics of chaotic system to encrypted color image [4]. Choquet fuzzy integral and piecewise linear of chaotic map were applied to encrypted color image [5]. Wei *et al.* [6] introduced a color image encryption scheme through DNA sequence operation and chaotic sequence. Kadir *et al.* represented a color image encryption algorithm by skew tent map and hyperchaotic system [7]. A new color image encryption algorithm is presented through Rhouma *et al.* [8]. Wu *et al.* designed a lossless color image encryption algorithm, the scheme by 6D hyperchaotic and plane-image to improve safety performance [9]. The image encryption scheme according to block confused and dynamic index diffused is introduced by Xu *et al.* [10]. These different image encryption algorithms [4]– [8], [10] just encrypted image, and not compress image, which bring high storage and transmission costs of the information. Because compression sensing (CS) can effectively compress and encrypt image, therefore, we propose a novel color image compression-encryption algorithm through CS to overcome these shortcoming.

Compared to other chaotic system, the fractional-order chaotic system possesses more abundant dynamics characteristics, because of its nonlocal features and high

The associate editor coordinating the review of this manuscript and approving it for publication was Sun Junwei.

nonlinearity [22]– [25]. What's more, the fractional-order chaotic system is used to cryptosystem, which increase the key space and improve security. The fractional-order memristive system is solved through Adomian decomposition method (ADM) algorithm [26]– [28], which reduces computation time and enhances space complexity. In addition, memristor chaotic system is easy to implement in practical application. Memristor, a nonlinear two-terminal electronic component was predicted by Chua [28]. It is used for construction chaotic oscillators through replacing linear or nonlinear resistance components [29]– [30]. Until 2008, the memristor was fabricated in I Iewlett-Packard Lab [33], which shown that the memristor was physically realized. After that, many new memristive chaotic systems were proposed and practical circuit could be realized [34]– [36]. Therefore, in this algorithm, we chose the fractional-order memristive chaotic circuit for image encryption.

In 2006, Candes and Donoho proposed CS theory. They proved that sample signal much smaller than the data sampling rate specified by Nyquist's theorem when the signal is sparse or compressible [37], and the high probability signal can be accurately reconstructed. To improve security and compression features of the image compression and encryption algorithm has been proposed, an improved algorithm by CS and 4D hyperchaotic system is proposed by Tong *et al.* [38]. Zhu *et al.* [39] designed a novel compression-encryption algorithm by 2D discrete hyperchaotic system, CS and Chinese remainder theorem. A color image encryption algorithm through CS and fractional Fourier transform is proposed [40]. Chai *et al.* [41] proposed a visually secure image encryption scheme based on compressive sensing. Among them, they just performed one time compression, which would not enough to cut short the storage and transmission costs of encrypted image. To adequately reduce the costs, our algorithm performs twice compression. In addition, the chaotic pseudo-random sequences were not tested randomness even though they used in these algorithms. In this paper, the randomness of chaotic pseudo-random sequences is tested by NIST SP800-22.

In this paper, we focus on investigating a color image compression-encryption algorithm through CS and fractional-order chaotic circuit. The rest of the paper is organized as follows. In Section 2, the basic definition and preliminary are introduced. In Section 3, dynamical behaviours of fractional-order memristive chaotic circuit are analyzed, and its pseudo-random sequences are designed and tested. The proposed algorithm is described in section 4. In section 5, the simulation results of the proposed algorithm are given. The security performances are analyzed in section 6. Finally some conclusions are obtained.

II. BASIC DEFINITION AND PRELIMINARY

A. COMPRESSION SENSING (CS)

Assumption one dimensional signal $y = [y(1), y(2), \ldots, y(N)]^{\mathrm{T}}$, the linear combination of its orthogonal basis is defined by

$$y = \Psi S = \sum_{i=1}^{N} S_i \Psi_i, \tag{1}$$

where Ψ, S are basis matrix, column vector, $N \times 1$ column vector and the sparse coefficient of y respectively. If S has K coefficients not equal to non-zero and (N-K) coefficients equal to zero, y is deemed to be sparse. The sparse signal y is measured through the measurement matrix $\Phi \in R^{M\times N}$, and the corresponding measured value Y is obtained by

$$\mathrm{Y} = \Phi y = \Phi\Psi S = \Theta S, \tag{2}$$

where Θ represents a $M \times N$ matrix.

The signal reconstruction is essentially a linear equation solving process. Because the number of unknowns is more than equations in Eq. (2) and the coefficients S are sparse, the Eq. (2) has a group of multiple solutions. The minimum norm l_0 to reconstruct signal can be solved, if the measurement matrix Φ and the basis matrix Ψ are meet to (Restricted Isometry Property) RIP [42]. For all $y \in \sum k$, the existing $\delta_k \in$(0,1) is used to:

$$(1 - \delta_k) \|y\|_2^2 \leq \|Ay\|_2^2 \leq (1 + \delta_k) \|y\|_2^2 , \tag{3}$$

where y is k-order sparse signal. δ_k is RIP constant, and matrix $A \in R^{M\times N}$ is meet k-order RIP.

The signal can be accurately reconstructed by

$$\hat{S} = \arg\min \|S\|_0, \quad s.t.\ Y = \Theta S \tag{4}$$

where $\|\cdot\|$ 0 is vector norm l_0, and it means that the amount of non-zero elements in the vector y.

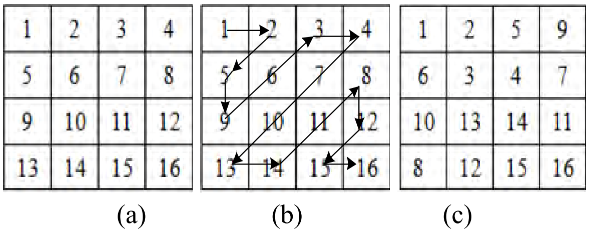
We use discrete cosine transform (DCT) to extend image pixel matrix. The measurement matrix is obtained by chaotic pseudo-random sequence and Hadamar matrix. The orthogonal matching pursuit (OMP) algorithm is applied to reconstruct image.

B. ZIGZAG CONFUSION

Zigzag confusion refers to the transformation process of starting from the upper left element of the matrix, scanning the element in the matrix in the order of Z, and reorganizing them into the same size matrix in line. It is also called the standard transformation. Generally, 4 × 4 or 8 × 8 sub-blocks are used as templates, or the whole square matrix can be scanned directly. For example, the zigzag confusion of a 4 × 4 matrix is shown in Fig. 1. Where the Fig. 1(a) is original matrix, the start pixel's position is (1, 1) of zigzag confusion process as shown in Fig.1 (b), and the result of matrix zigzag confusion is shown in Fig.1(c). From the Fig. 1, we can see that the matrix can be effectively scanned by zigzag confusion.

C. ADOMIAN DECOMPOSITION METHOD (ADM)

Suppose the fractional-order chaotic system $*D_{to}^{q}(\mathrm{t}) = f(x(t)) + g(t)$, here $x(t) =[x_1(t), x_2(\mathrm{t}), \ldots, x_n(\mathrm{t})]^{\mathrm{T}}$ are given



(a)

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

(b)

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

(c)

1	2	5	9
6	3	4	7
10	13	14	11
8	12	15	16

FIGURE 1. Zigzag confusion (a) original matrix, (b) zigzag confusion, (c) the matrix after zigzag confusion.

function variables, in autonomous systems, $g(t)$ =$[g_1(t)$, g_2(t),..., g_n(t)]$^{\mathrm{T}}$ are constants, $f(x(t))$ including linear and nonlinear partial functions. The system is divided into three parts by the following formulation [22],

$$\begin{cases} *D_{to}^{q}x(t) = Lx(t) + Nx(t) + g(t) & \\ x^{(k)}(t_0^{+}) = b_k, & k = 0, 1, \ldots, m-1 \\ m \in N, & m-1 < q \leq m, \end{cases} \tag{5}$$

where $^{*}D_{to}^{q}$ means that the derivative operator of order q, L represent the linear part of the system function and N is the non-linear part of system function, and b_k is initial value. By applying the J_{to}^{q} both sides of Eq. (3) and obtained following equation [23]:

$$x = J_{t0}^{q}Lx + J_{t0}^{q}Nx + J_{t0}^{q}g + \sum_{k=0}^{m-1} b_k \frac{(t-t_0)^k}{k!}, \tag{6}$$

where J_{to}^{q} represent the integral operator of order q, and $t_0 \leq t \leq t_1, q \geq 0, r \geq 0, \gamma > -1$ and C is real constant. The basic characteristics of the integral operator J q to are presented by [22]:

$$J_{t0}^{q}(t-t_0)^{\gamma} = \frac{\Gamma(\gamma+1)}{\Gamma(\gamma+1+q)}(t-t_0)^{\gamma+q}, \tag{7}$$

$$J_{t0}^{q}C = \frac{C}{\Gamma(q+1)}(t-t_0)^{q}, \tag{8}$$

$$J_{t0}^{q}J_{t0}^{r}x(t) = J_{t0}^{q+r}x(t). \tag{9}$$

According to principle of Adomian decomposition algorithm, the non-linear parts of Eq. (5) are decomposed by

$$\begin{cases} A_j^i = \dfrac{1}{i!}[\frac{d^i}{d\lambda^i}N(v_j^i(\lambda))]_{\lambda=0} \\ v_j^i(\lambda) = \sum_{k=0}^{i}(\lambda)^k x_j^k \end{cases}, \tag{10}$$

where, i $\in(0, \infty), j$ $\in(1, n)$. Then the non-linear parts are express as

$$Nx = \sum_{i=0}^{\infty} A^i(x^0, x^1, \ldots, x^i). \tag{11}$$

So the solution of Eq. (5) $x = \sum_{i=0}^{\infty}$ is described by

$$\begin{cases} x^0 = J_{t0}^{q}g + \sum_{k=0}^{m-1} b_k \dfrac{(t-t_0)^k}{k!} \\ x^1 = J_{t0}^{q}Lx^0 + J_{t0}^{q}A^0(x^0) \\ x^2 = J_{t0}^{q}Lx^1 + J_{t0}^{q}A^1(x^0, x^1) \\ \ldots \\ x^i = J_{t0}^{q}Lx^{i-1} + J_{t0}^{q}A^{i-1}(x^0, x^1, \ldots, x^{i-1}). \\ \ldots \end{cases} \tag{12}$$

III. FRACTIONAL-ORDER MEMRISTOR CHAOTIC CIRCUIT PSEUDO-RANDOM SEQUENCES

A. FRACTIONAL-ORDER CHAOTIC CIRCUIT

Here, the memristor chaotic circuit as shown in Fig. 2(a), the equivalent circuit of voltage-controlled memristor is shown in Fig. 2(b). On this basis, a fractional-order memristive chaotic circuit is defined.

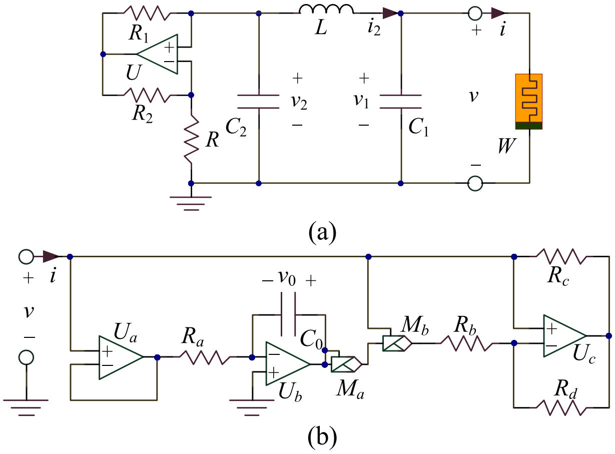


FIGURE 2. Memristor circuit based on Chua's circuit, (a) simple circuit schematic, (b) Voltage-controlled memristor circuit.

Based on Fig. 2(b), the relationship of input voltage v and current i, and voltage v_0 and capacitor C_0, are described as follows

$$C_0\frac{\mathrm{d}v_0}{\mathrm{d}t} = -\frac{1}{R_a}v, \tag{13}$$

$$i = W(v_0)v = -\frac{1}{R_b}(1 - gv_0^2)v, \tag{14}$$

where g represents overall gain of multipliers M_{a} and M_{b}.

For the variables v_0, v_1, v_2 and i in Fig. 2(a), the circuit equations are given by

$$\begin{cases} C_0\dfrac{\mathrm{d}v_0}{\mathrm{d}t} = -\dfrac{1}{R_a}v_1 \\ C_1\dfrac{\mathrm{d}v_1}{\mathrm{d}t} = \dfrac{1}{R_a}(1 - gv_0^2)v_1 + i_2 \\ C_2\dfrac{\mathrm{d}v_2}{\mathrm{d}t} = \dfrac{v_2}{R} - i_2 \\ L\dfrac{\mathrm{d}i_2}{\mathrm{d}t} = v_2 - v_1 \end{cases}, \tag{15}$$

where $v = v_1$.

Let $x = v_0, y = v_1, z = v_2, w = Ri_2, \tau = t/RC_2, R_b = R$, $a = RC_2/R_aC_0$, $b = C_2/C_1$, $c = R_2C2/_L$, so the Eq. (15) is defined as [43]

$$\begin{cases} \dot{x} = -ay \\ \dot{y} = b(1 - gx^2)y + bw \\ \dot{z} = z - w \\ \dot{w} = c(z - y) \end{cases}, \tag{16}$$

where a, b, c and g represent system parameters. Set $a = 12.375$, $b = 7.0213$, $c = 2.475$, $g = 0.2$ and $x \in (0, 1.5, 0, 0)$, we get the Lyapunov exponents (0.0805, 0, -0.0303, -34.5343). Obviously, in these Lyapunov exponent values, there is a positive exponent, which shows that the system is chaotic.

According to the fractional-order definition, and corresponding the fractional-order system is given by

$$\begin{cases} {}^cD^q_{t_0}x_1 = -ax_2 \\ {}^cD^q_{t_0}x_2 = b(1 - gx_1^2)x_2 + bx_4 \\ {}^cD^q_{t_0}x_3 = x_3 - x_4 \\ {}^cD^q_{t_0}x_4 = c(x_3 - x_2) \end{cases}, \tag{17}$$

where q represent order of the equation. When $q = 1$, system (17) becomes system (16).

B. THE SOLUTION OF FRACTIONAL-ORDER MEMRISTOR CHAOTIC CIRCUIT

The fractional-order system (17) is derived by ADM algorithm, and then linear and nonlinear terms are obtained as follows

$$\begin{bmatrix} L_{x1} \\ L_{x2} \\ L_{x3} \\ L_{x4} \end{bmatrix} = \begin{bmatrix} -ax_2 \\ bx_2 + bx_4 \\ x_3 - x_4 \\ c(x_3 - x_2) \end{bmatrix}, \begin{bmatrix} N_{x1} \\ N_{x2} \\ N_{x3} \\ N_{x4} \end{bmatrix} = \begin{bmatrix} 0 \\ -bgx_1^2x_2 \\ 0 \\ 0 \end{bmatrix}. \tag{18}$$

Based on Eq. (10), the before five Adomian polynomials for the nonlinear part -bg $x_1^2x^2$ are

$$\begin{cases} A^0{}_{-bgx_2(x_1)^2} = -bgx_2^0(x_1^0)^2 \\ A^1{}_{-bgx_2(x_1)^2} = -bg(x_2^1(x_1^0)^2 + 2x_2^0x_1^1x_1^0) \\ A^2{}_{-bgx_2(x_1)^2} = -bg(x_2^2(x_1^0)^2 + 2x_2^1x_1^1x_1^0 + 2x_2^0x_1^2x_1^0 + x_2^0(x_1^1)^2) \\ A^3{}_{-bgx_2(x_1)^2} = -bg(x_2^3(x_1^0)^2 \\ \qquad +2(x_2^2x_1^0x_1^1 + x_2^0x_1^3x_1^0 + x_2^0x_1^1x_1^2)) \\ \qquad -bg(2x_2^1x_1^2x_1^0 + x_2^1(x_1^1)^2) \\ A^4{}_{-bgx_2(x_1)^2} = -bg(x_2^4(x_1^0)^2 \\ \qquad +2(x_2^3x_1^0x_1^1 + x_2^2x_1^2x_1^0 + x_2^1x_1^1x_1^2)) \\ \qquad -2bg(2(x_2^1x_1^3x_1^0 + x_2^0x_1^4x_1^0 + x_2^0x_1^3x_1^0) + x_2^2(x_1^1)^2 \\ \qquad +x_2^0(x_1^2)^2) \end{cases} \tag{19}$$

The initial conditions are

$$\begin{cases} x_1^1 = -ax_2^0\dfrac{(t - t_0)^q}{\Gamma(q + 1)} \\ x_2^1 = (b(x_2^0 - gx_2^0(x_1^0)^2) + bx_4^0)\dfrac{(t - t_0)^q}{\Gamma(q + 1)} \\ x_3^1 = (x_3^0 - x_4^0)\dfrac{(t - t_0)^q}{\Gamma(q + 1)} \\ x_4^1 = (b(x_3^0 - x_2^0))\dfrac{(t - t_0)^q}{\Gamma(q + 1)} \end{cases}, \tag{20}$$

where x_j^0 is the initial values of system (17), $h = t - t_0$, and then the solution of system (17) can be represented by

$$\tilde{x}_j(t) = c_j^0 + c_j^1\frac{(t - t_0)^q}{\Gamma(q + 1)} + c_j^2\frac{(t - t_0)^{2q}}{\Gamma(2q + 1)} + c_j^3\frac{(t - t_0)^{3q}}{\Gamma(3q + 1)} + c_j^4\frac{(t - t_0)^{4q}}{\Gamma(4q + 1)} \tag{21}$$

where

$$\begin{cases} c_1^0 = x_1^0 \\ c_2^0 = x_2^0 \\ c_3^0 = x_3^0 \\ c_4^0 = x_4^0 \end{cases}, \tag{22}$$

$$\begin{cases} c_1^1 = -ac_2^0 \\ c_2^1 = bc_2^0 + bc_4^0 - bgc_2^0(c_1^0)^2 \\ c_3^1 = c_3^0 - c_4^0 \\ c_4^1 = c(c_3^0 - c_2^0) \end{cases}, \tag{23}$$

$$\begin{cases} c_1^2 = -ac_2^1 \\ c_2^2 = bc_2^1 + bc_4^1 - bg(c_2^1(c_1^0)^2 + 2c_2^0c_1^1c_1^0) \\ c_3^2 = c_3^1 - c_4^1 \\ c_4^2 = c(c_3^1 - c_2^1) \end{cases}, \tag{24}$$

$$\begin{cases} c_1^3 = -ac_2^2 \\ c_2^3 = bc_2^2 + bc_4^2 - bg(c_2^2(c_1^0)^2 + 2c_2^0c_1^2c_1^0 \\ +(2c_2^1c_1^1c_1^0 + c_2^0(c_1^{11})^2))\dfrac{\Gamma(2q + 1)}{\Gamma^2(q + 1)} \\ c_3^3 = c_3^2 - c_4^2 \\ c_4^3 = c(c_3^2 - c_2^2) \end{cases}, \tag{25}$$

$$\begin{cases} c_1^4 = -ac_2^3 \\ c_2^4 = bc_2^3 + bc_4^3 - bg((c_2^2(c_1^0)^2 + 2c_2^0c_1^3c_1^0 \\ +2(c_2^2c_1^1c_1^0 + c_2^1c_1^2c_1^0 + c_2^0c_1^1c_1^2)\dfrac{\Gamma(3q + 1)}{\Gamma(q + 1)\Gamma(2q + 1)} \\ +c_2^3(c_1^{11})^2\dfrac{\Gamma(3q + 1)}{\Gamma^3(q + 1)}) \\ c_3^4 = c_3^3 - c_4^3 \\ c_4^4 = c(c_3^3 - c_2^3). \end{cases} \tag{26}$$

C. DYNAMICAL ANALYSIS OF FRACTIONAL-ORDER CHAOTIC CIRCUIT

Here, set the system parameter $a = 12.375$, $b = 7.0213$, $c = 2.475$, $g = 0.2$, $q = 0.98$, $h = 0.001$ and initial values (x_1, x_2, x_3, x_4)$\in$ (0, 1.5, 0, 0), and we get Lyapunov exponents

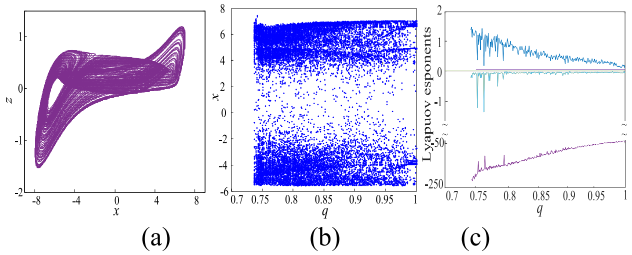


FIGURE 3. Dynamic characteristics of the fractional-order memristor chaotic system, (a) x-y plane, (b) bifurcation diagram for q ∈(0.7, 1), (c) Lyapunov exponents spectrum for q∈(0.7, 1).

(0.1209, 0, -0.0580, -49.9689), Lyapunov dimension $D_{\mathrm{L}} = 3.0013$ and phase diagram as shown in Fig.3 (a).Therefore, the system is chaotic. Then let the other parameters and initial values keep unchanged, order $q \in (0.7, 1)$, bifurcation diagram and Lyapunov exponents spectrum are shown Fig.3 (b) and (c). From the Fig. 3(b) and (c), we can see that the fractional-order memristor chaotic circuit system has better randomness and parameters sensitivity. Hence, it can improve security performance to apply in image encryption algorithm.

D. DESIGN OF FRACTIONAL-ORDER CHAOTIC PSEUDO-RANDOM SEQUENCE

The quantized sequences of chaotic sequences are called chaotic pseudo-random sequences. The randomness of chaotic system is mostly reflected in the performance of quantized random sequences. Quantization of chaotic real value sequence is an important part of generating pseudo-random sequence design. This process directly affects the randomness, complexity and other characteristics of sequences, and ultimately affects the security of its application system. Set $a = 12.375$, $b = 7.0213$, $c = 2.475$, $g = 0.2$, initial system value $(x_1, x_2, x_3, x_4) \in (0, 1.5, 0, 0)$, then the system are decimals as the chaotic sequences. The specific steps as follows.

Step 1: After the system parameters and initial values are determined, the system was iterated for 5000 times to eliminate the transient effect, and then fractional-order memristive chaotic circuit system is continued to be iterated. We get the four decimals sequences, and then new four decimals sequences are generated by

$$\begin{cases} xl(j) = 2 \times x(j) - \dfrac{\max(x) + \min(x)}{\max(x) - \min(x)} \\ y1(j) = 2 \times y(j) - \dfrac{\max(y) + \min(y)}{\max(y) - \min(y)} \\ z1(j) = 2 \times z(j) - \dfrac{\max(z) + \min(z)}{\max(z) - \min(z)} \\ wl(j) = 2 \times w(j) - \dfrac{\max(w) + \min(w)}{\max(w) - \min(w)}, \end{cases} \tag{27}$$

where $x(j)$, $y(j)$, $z(j)$ and $w(j)$ represents four chaotic sequences, max and min are Maximum and Minimum of chaotic sequence. In addition, $x1(j)$, $y1(j)$, $z1(j)$ and $w1(j)$ denote new decimals sequences.

Step 2: Decimals sequences are converted to integer sequence by taking the module, integer up and integer down.

$$\begin{cases} x2(j) = \mathrm{mod}(\mathit{round}(1000 \times |x1(j) \times 10^{16}| \\ \qquad -\mathit{floor}(|x1(j) \times 10^{16}|)) \\ y2(j) = \mathrm{mod}(\mathit{round}(1000 \times |y1(j) \times 10^{16}| \\ \qquad -\mathit{floor}(|y1(j) \times 10^{16}|)) \\ z2(j) = \mathrm{mod}(\mathit{round}(1000 \times |z1(j) \times 10^{16}| \\ \qquad -\mathit{floor}(|z1(j) \times 10^{16}|)) \\ w2(j) = \mathrm{mod}(\mathit{round}(1000 \times |w1(j) \times 10^{16}| \\ \qquad -\mathit{floor}(|w1(j) \times 10^{16}|)) \end{cases}, \tag{28}$$

where $x1(j)$, $y1(j)$, $z1(j)$, $w1(j)$ represents new four decimals sequences, and $x2(j)$, $y2(j)$, $z2(j)$, $w2(j)$ denote new integer sequences.

E. NIST SP800-22 TEST

In this paper, the quantized chaotic pseudo-random sequences are used to image compression and encryption algorithm, and random sequence performance is analyzed by NIST SP800-22. For this test, all testing is done automatically through the test package STS. There are 15 test indicators and 2 kinds of judgment basis (P-value, pass rate) in NIST SP800-22 [44]. For the pass rate, given significant level of α, test sequence β group, the confidence interval of pass-through rate is defined as:

$$(1 - \alpha - 3\sqrt{\alpha(1-\alpha)/\beta},\ 1 - \alpha + 3\sqrt{\alpha(1-\alpha)/\beta}). \tag{29}$$

If the pass rate falls within this confidence interval, which indicates that the sequence passed the test, otherwise, the test is failed. For P-value, if $P\text{-value} > 0.0001$, which shows that the sequence is random, otherwise, the sequence is not random.

Setting the significant level of $\alpha = 0.01$, test sequence $\beta = 100$, each group leader is 1 000 000 bit, the confidence interval is [0.96, 1], we get the pseudo-random sequences of test results for fractional-order memristor chaotic circuit as shown in Table.1. From the Table.1 we can see that the pseudo-random sequence generated by fractional-order memristive chaotic circuit passed 15 test indexes of NIST SP 800-22 random number inspection standard. Moreover, the image encryption algorithm using fractional-order memristor chaotic circuit has more high security features.

IV. IMAGE COMPRESSION-ENCRYPTION AND DECRYPTION ALGORITHM

A. COMPRESSION-ENCRYPTION ALGORITHM

The proposed color image compression and encryption algorithm process is shown in Fig.4, and the main process is consist of decomposition of the image plane, discrete cosine transform (DCT), CS, Zigzag scrambling and add modulus and BitCircShift diffusion. The details of compression and encryption scheme are as follows.

Step 1: The plain color image I with size of $H \times W$ is inputted.

TABLE 1. Test Results Of NIST SP 800-22.

The test serial number	The test name	P-value	Pass rate	Test number	Test results
1	Frequency	0.867692	0.99	1	success
2	Block Frequency	0.77918	1	1	success
3	Cumulative Sums (*)	0.739918	0.99	2	success
4	Runs	0.779188	0.98	1	success
5	Longest Run	0.055361	1	1	success
6	Rank	0.474986	0.99	1	success
7	FFT	0.062821	1	1	success
8	Non-overlapping Template(*)	0.071177	0.99	148	success
9	Overlapping Template	0.013569	0.99	1	success
10	Universal	0.108791	0.99	1	success
11	Approximate Entropy	0.759756	1	1	success
12	Random Excursions (*)	0.249284	0.98	8	success
13	Random Excursions Variant(*)	0.025193	0.98	18	success
14	Serial(*)	0.137282	0.98	2	success
15	Linear Complexity	0.224821	0.97	1	success

Where, *tests contain multiple tests, listed as the worst case.

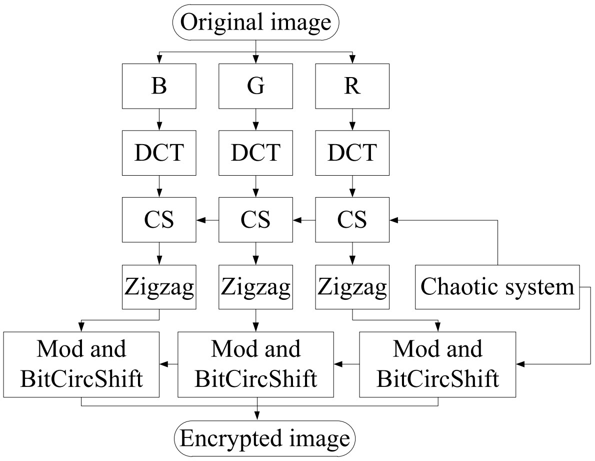


FIGURE 4. Flowchart of the process encryption algorithm.

Step 2: The plain color image I are decomposed into three plains R, G and B with size of $H \times W$.

Step 3: To sparse the pixel matrix of image, three sparse matrices of planes R, G and B are obtained by DCT operation. The definition of DCT is as follows,

$$B_{pq} = \alpha_p \alpha_q \sum_{h=0}^{H-1} \sum_{w=0}^{W-1} A_{hw} \cos \frac{\pi(2h+1)p}{2H} \cos \frac{\pi(2w+1)q}{2w}, \tag{30}$$

where, * tests contain multiple tests, listed as the worst case.

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{H}}, \ p = 0 \\ \sqrt{\frac{2}{H}}, \ 1 \leq p \leq H-1 \end{cases}, \tag{31}$$

$$\alpha_q = \begin{cases} \frac{1}{\sqrt{W}}, \ q = 0 \\ \sqrt{\frac{2}{W}}, \ 1 \leq q \leq W-1 \end{cases}, \tag{32}$$

where A is pixel matrix of original image, and B represents the new matrix, H and W means that the length and height of the image.

Step 4: To get the measurement matrix, for the fractional-order memristor chaotic circuit system, setting the parameter and initial values, let the system (20) iterate $m + M$ times and thrown away the former m values to enhance initial value sensitivity. We obtain four chaotic sequences, and then the four pseudo-random sequences are obtained by quantization operation of chaotic sequences, the quantitative principle is defined in section III D.

Step 5: Three pseudo-random sequences are randomly selected from the Step.4, and then three measurements matrices of $M \times M$ are obtained by combining the Hadamar matrix and $M = CR$(compression ratio) $\times$ H. Here, Hadamar matrix is generated by

$$\begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} \tag{33}$$

Step 6: According to mensurement, three sparse plain matrices after DCT is calculated by compression using three measurement matrices. We get three compressed image pixel matrices $H \times M$, on the basis of this, by calculating the second mensurement matrix. Then three compressed image pixel matrices $M \times M$ are obtained.

Step 7: The confusion operations of the three compressed pixel matrices. The pixel positions of three compressed image pixel matrices are scrambled by the zigzag confusion in Section 2.2, and we can get three confused image pixel matrices.

Step 8: In order to obtain the random of chaotic sequence of diffusion operations, setting parameters and initial conditions of the fractional-order memristor chaotic circuit system, and let the system (20) iterate $n + M$ times and thrown away the former n values to enhance initial value sensitively, we can

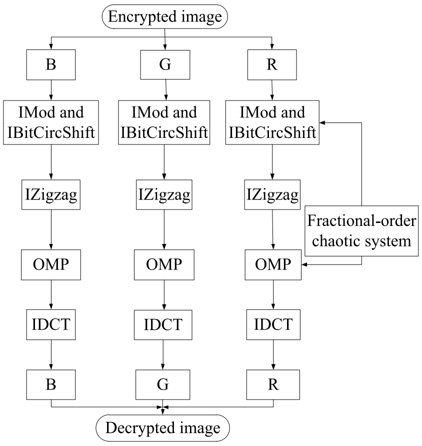


FIGURE 5. Flowchart of the process decryption algorithm.

get four chaotic sequences, and then four pseudo-random sequences are generated by Eq. (27) and Eq. (28).

Step 9: In diffusion operations, the pixel values are diffused by new pseudo-random sequence. The new two pseudo-random sequences S_1 and S_2 are obtained by

$$\begin{cases} p(4j-3) = x(j) \\ p(4j-2) = y(j) \\ p(4j-1) = z(j) \\ p(4j) = w(j) \end{cases}, \tag{34}$$

where $x(j)$, $y(j)$, $z(j)$ and $w(j)$ represent four pseudo-random sequences, and p represent new pseudo-random sequence.

Step.10 The diffusion operations for three scrambled image pixel matrices are performed through the Modularization and the BitCircShift algorithm. The diffusion results are obtained by

$$\begin{cases} C_i = (C_{i-1} \oplus S_i \oplus P_i) <<< LSB_3\,(C_{i-1}) \\ C_i = (C_{i-1} + S_i + P_i) \bmod 256 <<< LSB_3\,(C_{i-1})\,, \end{cases} \tag{35}$$

where S_i are the pseudo-random sequences S1 and S2. LSB_3 represents the lowest three digits of the data, and the proposed algorithm using the 8b image, therefore, each pixel has 8b, the lowest three digits of the any one data is (0, 7). This is the valid range of circular bits for a pixel point data.

Step 11: The encrypted image is obtained through combining three diffused image pixel matrices.

B. DECRYPTION ALGORITHM

It is obvious from the Fig.5 that decryption algorithm process including the Modularization and the BitCircShift, Zigzag and DCT inverse algorithm. A detailed process of the reconstruction and decryption algorithm is presented as follows.

Step 1: For an encrypted image $M\times M$, decompose it into three pixel matrices $M\times M$.

Step 2: The Modularization and the BitCircShift inverse algorithm are used to recover three diffused pixel matrices. The diffusion pseudo-random sequences are obtained by Step.8 and 9 of the encryption.

Step 3: Three compressed pixel matrices are regained through Zigzag reverse algorithm.

Step 4: Three sparse plane matrices $N \times N$ are reconstructed based on OMP algorithm. Where, the measurement matrices are generated by using Eq. (30) and (31).

Step 5: The decryption image is obtained by DCT inverse algorithm and IDCT is calculated as follow

$$A_{mn} = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \tag{36}$$

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le p \le M-1 \end{cases}, \tag{37}$$

$$\alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \le q \le N-1 \end{cases}, \tag{38}$$

where B represents the pixel matrix reconstructed by OMP algorithm. A denote new IDCT result matrix, M and N means that length and height of the image.

V. SIMULATION RESULTS

A. THE RESULTS OF ENCRYPTION AND DECRYPTION ALGORITHMS

Setting the parameters $a = 12.375$, $b = 7.0213$, $c = 2.475$, $g = 0.2$, $h = 0.001$, $q = 0.98$, $x_0 = 0$, $y_0 = 1.5$, $z_0 = 0$, $w_0 = 0$, $m = 500$ and $n = 500$, and then input color "Lena" and "pepper" images with the size of 256 × 256. The proposed compression and encryption algorithm are performed in MATLAB 2014a, and the compression ratio is 0.8, the encrypted image and decrypted image are as shown in Fig. 6. It can be seen from the Fig. 6 that the new algorithm can compression and encryption image effectively.

B. THE COMPRESSION RATIO ANALYSIS

The compression performance of the new algorithm is analyzed by Mean Structural Similarity (MSSIM) and Peak Signal to Noise Ratio (PSNR) with different compression ratios (CR). TheCR is defined as [45];

$$CR = \frac{C_M \times C_N}{I_M \times I_N}, \tag{39}$$

where I_M and I_N are length and height of original image. C_M and C_N are length and height of encrypted image, respectively.

1) MEAN STRUCTURAL SIMILARITY (MSSIM)

The MSSIM is used to estimate the characteristic of the encryption algorithm, and it is described by [46]

$$l(X, Y) = \frac{2\mu_X\mu_Y + L_1}{\mu_X^2 + \mu_Y^2 + L_1}, \tag{40}$$

$$c(X, Y) = \frac{2\sigma_X\sigma_Y + L_2}{\sigma_X^2 + \sigma_Y^2 + L_2}, \tag{41}$$

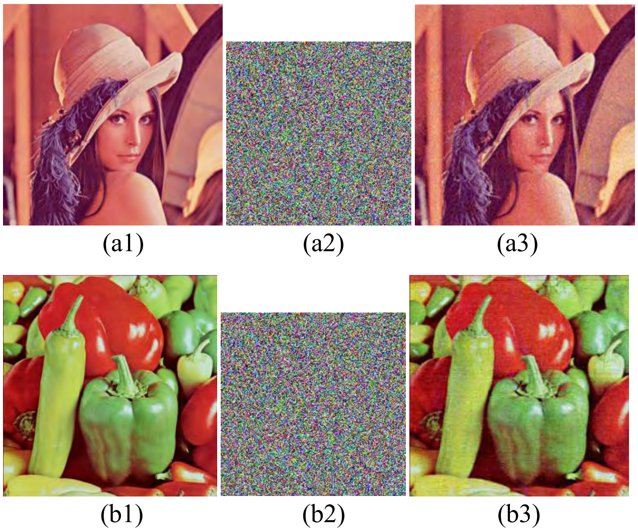


FIGURE 6. Algorithm test results, (a1) original Lena image, (a2) encrypted Lena image, (a3) decrypted Lena image, (b1) original pepper image, (b2) encrypted pepper image, (b3) decrypted pepper image.

$$s(X,Y)=\frac{\sigma_{XY}+L_3}{\sigma_X\sigma_Y+L_3}, \tag{42}$$

$$\mathrm{SSIM}(X,Y)=l(X,Y)\times c(X,Y)\times s(X,Y), \tag{43}$$

$$\mathrm{MSSIM}(X,Y)=\frac{1}{M}\sum_{k=1}^{M}\mathrm{SSIM}\left(x_k,y_k\right), \tag{44}$$

where μ represent the mean of image structural. σ means that image variance structural. L_1, L_2 and L_3 represent small constants to avoid denominator of 0. M represent the overall number of image blocks. Here, parameters $L_1=(K_1\times C)^2$, $L_2=(K_2\times C)^2$, $L_3=L_2/2$, $K_1=0.001$, $K_2=0.003$, $M=64$, $C=255$. The MSSIM values with different CR are shown in Table.2. According to the Table.2, the MSSIM values change when the compression ratio varies, which effectively compress and encrypt image according to different practical application needs.

TABLE 2. Mssim Values Under The Different CR.

	Lena			pepper		
CR	R	G	B	R	G	B
0.8	0.7135	0.6551	0.4931	0.7410	0.6437	0.5112
0.4	0.4478	0.4135	0.4594	0.5191	0.4282	0.5388
0.2	0.3290	0.3456	0.3461	0.3563	0.2759	0.3375

2) PEAK SIGNAL TO NOISE RATIO (PSNR)

PSNR is used to evaluate the performance of reconstruction algorithm to restore image. The formula for calculating PSNR is defined as [46], [47]:

$$MSE=\frac{1}{rc}\sum_{i=1}^{r}\sum_{j=1}^{c}(E_{ij}-e_{ij})^2, \tag{45}$$

$$PSNR=\log_{10}(\frac{255^2}{MSE}), \tag{46}$$

where r and c are length and height of the image, MSE means that mean error between the original and the restore image. E_{ij} and e_{ij} are pixels of original and restore image in (i,j) position. The larger of PSNR value shows that the reconstructed image is closer to the original image. The PSNR values of different CR are listed in Table.3. The PSNR values are close to 30 when CR>0.4. Therefore, the reconstruction result is also good for a small of compression.

TABLE 3. Psnr values under the different CR.

	Lena			pepper		
CR	R	G	B	R	G	B
0.8	33.370	31.966	30.921	33.787	31.765	30.479
0.4	30.092	29.581	30.409	30.635	28.184	30.381
0.2	28.990	28.627	29.273	29.206	28.434	28.685

VI. PERFORMANCE ANALYSIS

For the security performance analysis of existing image encryption algorithms, Lena image is generally used as the target image for performance analysis. In order to facilitate comparison, we only analyze the features of Lena image.

A. KEY SPACE

For a good encryption algorithm, it should be has enough large key space and to resist brute force attacks. Our key of image compression and encryption scheme is comprised of chaotic system parameters a, b, c, g, q, h, initial values x_0, y_0, z_0, w_0, iterations m and n. If the computational accuracy is 10^{-15}, the key space of the proposed algorithm would be 2^{448}, which shows that the new algorithm has larger key space and can prevent the brute force attacks. Key space compared results with other algorithms as shown Table.4.

TABLE 4. Key space of different algorithm.

Our algorithm	Ref.[5]	Ref.[6]	Ref.[11]	Ref.[14]	Ref.[19]
2^{448}	2^{324}	2^{233}	2^{148}	2^{256}	2^{280}

B. KEY SENSITIVITY ANALYSIS

The sensitively is an important indicator to evaluate the security performance of encryption algorithm. To test the key sensitivity, we make a small change in the value of the secret key, the decrypted image results as Fig.7. It can be seen that if the key value is slightly changed, the decrypted image is entirely different from the original Lena image. Moreover, the proposed algorithm is extremely sensitivity to its key.

C. STATISTICAL ANALYSIS

In this section, the statistical performance is analyzed by histogram and the correlation coefficient.

1) HISTOGRAM ANALYSIS

The histogram indicates that the image pixel distribution. For the original image, its pixel distribution fluctuate, on the contrary, the encrypted image's pixel distribution is uniform

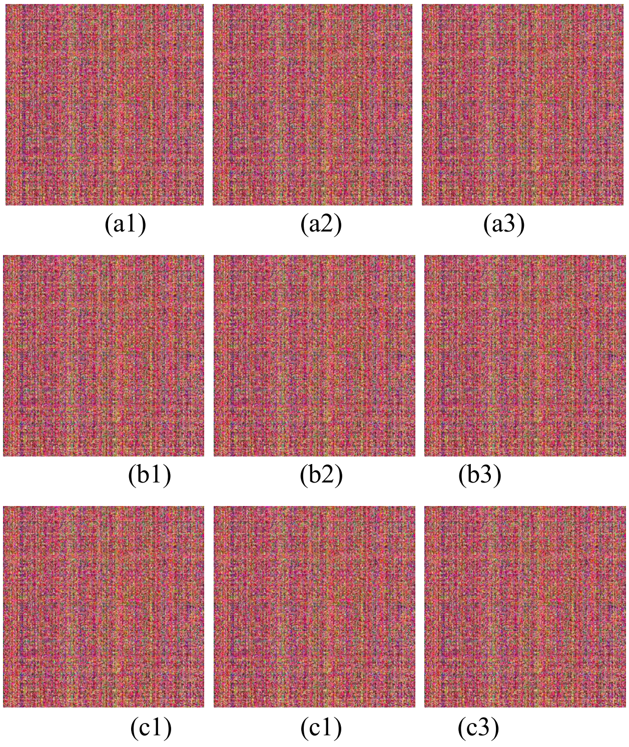


FIGURE 7. key sensitively test, (a1) $x0 + 10 - 15$, (a2) $y0 + 10 - 15$, (a3) $z0 + 10 - 15$, (b1) $w0 + 10 - 15$, (b2) $a + 10 - 15$, (b3) $b + 10 - 15$, (c1) $c + 10 - 15$, (c2) $g + 10 - 15$, (c3) $q + 10 - 15$.

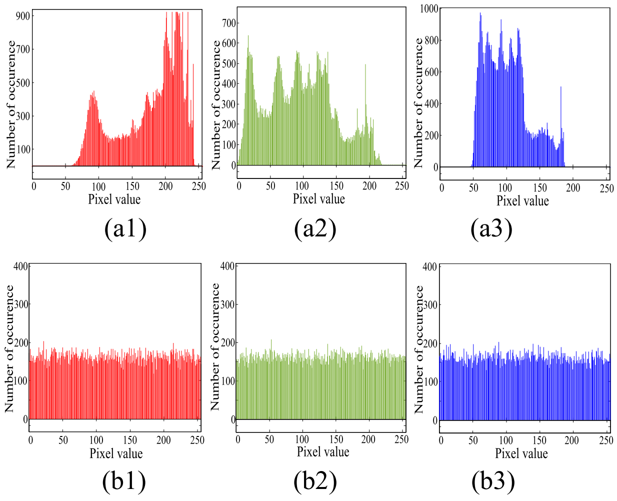


FIGURE 8. Histogram of image, (a1) histogram of original image R, (a2) histogram of original image G, (a3) histogram of original image B, (b1) histogram of encrypted image R, (b2) histogram of encrypted image G, (b3) histogram of encrypted image B.

and flat. The histogram of original and encrypted Lena image with R, G and B are represented in Fig.8. It shows that the histogram distribution of original image is fluctuates, histogram distribution of encrypted image is flat. Moreover, the proposed algorithm can resist histogram attack.

2) CORRELATION COEFFICIENT ANALYSIS

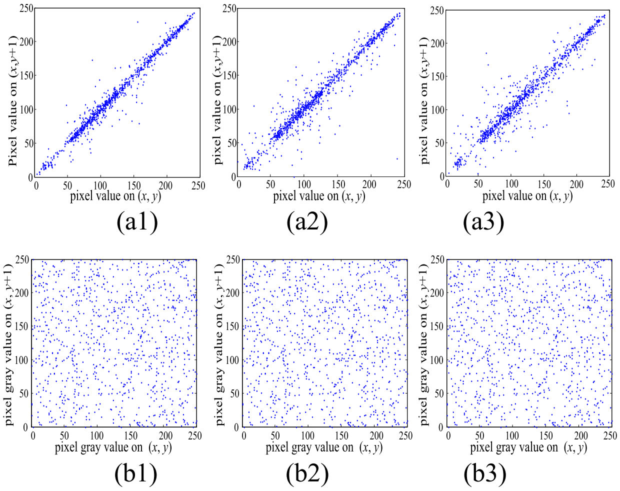


FIGURE 9. Correlation of images, (a1) correlation of original Lena image at horizontal, (a2) correlation of original Lena image at vertical, (a3) correlation of original Lena image at diagonal, (b1) correlation of encrypted Lena image at horizontal, (b2) correlation of encrypted Lena image at vertical, (b3) correlation of original Lena image at diagonal.

TABLE 5. Correlation coefficient of different directions.

Directions	Original image	Our algorithm	Ref.[4]	Ref.[5]	Ref.[6]
Horizontal	0.9824	0.0016	0.1257	0.0024	0.0044
Vertical	0.9632	0.0015	0.0581	0.0580	0.0034
Diagonal	0.9484	-0.0017	0.0504	0.0170	0.0020

Image correlation means that an important statistical characteristic of image, the encryption algorithm can be cracked through statistical analysis. Therefore, in this paper, the correlation coefficient of different pixels is used to measure the ability to reduce correlation of the algorithm. If the correlation coefficient of encrypted image is smaller than original image, the encryption performance of algorithm is good and the ability of anti-attack cracking is strong. Correlation coefficients of different pixels are calculated by [48]

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)D(y)}}, \tag{47}$$

where cov (x, y) represent the covariance of x and y, $D(x)$ and $D(y)$ means that variance of x and y. According to mathematical expectation $E(x)$, cov (x, y), $D(x)$ and $D(y)$ are calculated by

$$cov(x, y) = E\left\{[x - E(x)]\,[y - E(y)]\right\}, \tag{48}$$

$$E(x) = \frac{1}{M}\sum_{i=1}^{M} x_i, \tag{49}$$

$$D(x) = \frac{1}{M}\sum_{i=1}^{M} [x_i - E(x)]^2, \tag{50}$$

where M represent the overall pixels of the image. In the test, 1000 pixel pairs were randomly selected for the original Lena and Fig. 6(b), and the correlation coefficients of all directions were obtained by the above formulas. The correlations of original and encrypted Lena image at different directions are shown in Fig.9. The different pixel values of the original

TABLE 6. Correlation Coefficient of Different Direction for R, G and B.

Channels	Directions	Original image	Our algorithm	Ref.[9]	Ref.[19]
R	Horizontal	0.9774	-0.0020	-0.0206	0.0024
	Vertical	0.9553	-0.0013	-0.0116	0.0010
	Diagonal	0.9324	-0.0059	-0.0097	-0.0147
G	Horizontal	0.9706	-0.0022	-0.0005	-0.0056
	Vertical	0.9443	-0.0041	0.0002	-0.0037
	Diagonal	0.9194	0.0014	0.0189	-0.0295
B	Horizontal	0.9569	0.0069	0.0016	-0.0078
	Vertical	0.9721	0.0059	0.0133	0.0031
	Diagonal	0.9015	0.0035	-0.0123	-0.0247

image are distributed on the diagonal, which indicates that it has extremely correlation between adjacent pixels of original image. We can see that all the pixels of the encrypted image are distributed in the entire plane, which demonstrates that almost not have correlation between different pixels of encrypted image.

Correlation coefficient values of original and encrypted Lena image at different directions are listed in Table. 5. Correlation coefficient values between pixels of R, G and B components at different directions are shown in Table 6. We can see that correlation coefficient values of original image are about 1, the encrypted image are almost 0, which shows that the new algorithm can effectively reduce correlation between adjacent pixels of original image. Compared with other algorithms, the proposed color image compression and encryption scheme has higher security.

D. INFORMATION ENTROPY

The information entropy is a particularly useful measure to test the randomness of image information, and it is calculated by

$$H = -\sum_{j=0}^{M} p(i)\log_2 p(j), \tag{51}$$

where M means that the gray scale of the image, and $p(j)$ represent the probability of gray value j occurrence. For $L = 256$ gray image, the theoretical value of information entropy H is 8 [27]. The information entropy values of encrypted Lena image for R, G and B in Table 7. Table 8 listed the information entropy values of different encryption algorithms. From the Table 7 and 8 we can see that new algorithm has more randomness of image information.

E. DIFFERENTIAL ATTACK ANALYSIS

Researchers usually use pixel count change rate (NPCR) and average intensity change rate (UACI) as two criteria to measure whether the method can resist differential attack. NPCR and UACI calculation as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{L} \times 100\% \tag{52}$$

TABLE 7. Information entropy of R, G and B.

Images	R	G	B
Lena	7.9948	7.9958	7.9950
Ref.[7]	7.9729	7.9744	7.9705
Ref.[8]	7.9732	7.9750	7.9715
Ref.[9]	7.9914	7.9907	7.9907
Ref.[19]	7.9893	7.9898	7.9894

$$UACI = \frac{1}{L}\sum_{i,j} \frac{|C(i,j) - C_1(i,j)|}{256} \times 100\%, \tag{53}$$

here, C is encrypted image pixel value before original image changed, and C_1 is encrypted image pixel values after original image changed, L is the number of all pixels in an image, if $C(i,j)$ and $C_1(i,j)$ are not equal, then $D(i,j)$ is 1, otherwise $D(i,j)$ is 0.

In our experiments, we only change the lowest bit of one random pixel of the original image, and carry out the test for 10 times with one round of encryption to obtain the average NPCRs and UACIs as listed in Table.9. The results shows that the mean NPCRs and UACIs of our algorithm are over 99.6% and 33.3% respectively only through one round of encryption, which shows that the algorithm can prevent the differential attack.

F. ROBUSTNESS ANALYSIS

The robustness is an important measure to evaluate algorithm security. Image robustness refers to that the image still has certain fidelity after experiencing various signal processing or various attacks. In this test, robustness is analyzed by cropping attack, rotation attack.

1) CROPPING ATTACK

To test the algorithm resist cropping attack, we make the encrypted Lena image with six different data losses as shown in Fig. 10 (a), (b), (c), (d), (e) and (f). The corresponding decrypted images are presented in Fig. 10 (g), (h), (i), (j), (k) and (l), respectively. The Fig. 10 shows that even though the encrypted images are lost, the main information of image

TABLE 8. Information entropy of different encryption algorithm.

Algorithms	Our algorithm	Ref.[10]	Ref.[11]	Ref.[12]	Ref.[13]
Lena	7.9985	7.9973	7.9972	7.9879	7.9888

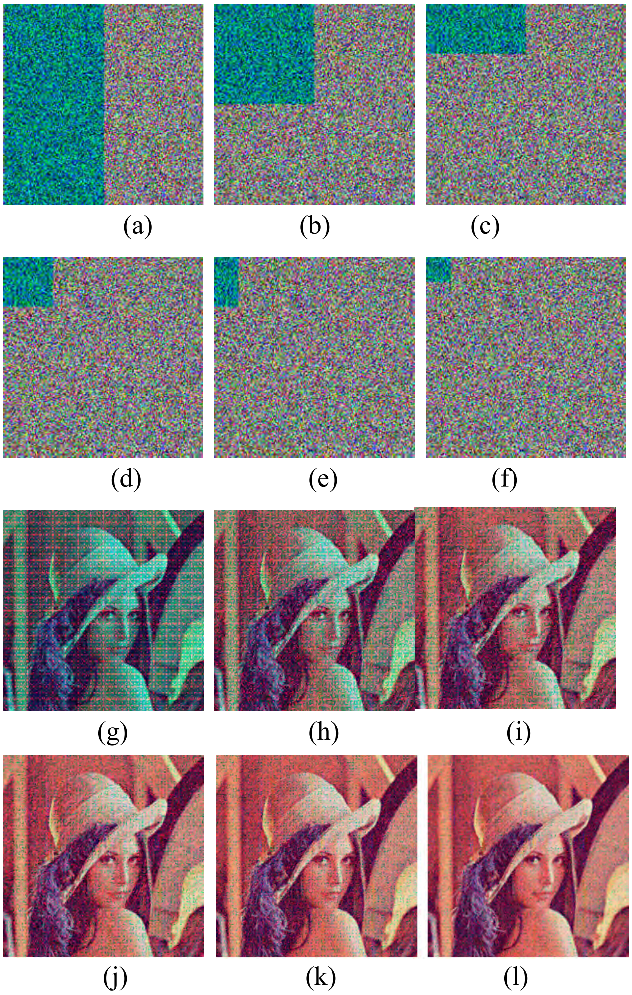


FIGURE 10. Cropping attack analysis results, (a) 1/2 data loss of Figure.6(a2), (b) 1/4 data loss of Figure.6(a2), (c) 1/8 data loss of Figure.6(a2), (d) 1/16 data loss of Figure.6(a2), (e) 1/32 data loss of Figure.6(a2), (f) 1/32 data loss of Figure.6(a2), (g) decrypted image of 1/2 data loss, (h) decrypted image of 1/4 data loss, (i) decrypted image of 1/8 data loss, (j) decrypted image of 1/16 data loss, (k) decrypted image of 1/32 data loss, (l) decrypted image of 1/64 data loss.

TABLE 9. Mean NPCRs and UACIs of encrypted Lena images.

Algorithms	*NPCR* (%)			*UACI* (%)		
Channel	*R*	*G*	*B*	*R*	*G*	B
Our	99.60	99.61	99.61	33.45	33.43	33.41
Ref [4]	99.42	99.60	99.54	27.78	27.66	24.94
Ref [6]	99.59	99.22	98.85	33.48	33.46	33.27

can be covered. Therefore, our algorithm would resist data loss attack in different degree.

2) ROTATION ATTACK

The rotation attack is a typical geometric attack. If the attacker made slight geometric transformation on the encrypted image, the pixel position in the image is almost completely changed, which make the image owner unable to get the properly encrypted image. For this test, the cipher image is rotated with 2°, 18° and 25°, and the test results as show in Fig. 11. The test results indicate that the algorithm can resist rotation attack.

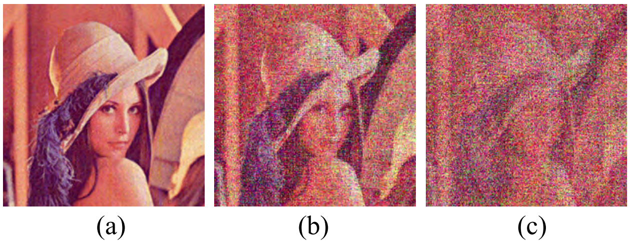


FIGURE 11. Rotation attack results, (a) recovered image of rotation 2°, (b) recovered image of rotation 18°, (c) recovered image of rotation 25°.

VII. CONCLUSION

In this paper, a fractional-order memristor chaotic circuit is obtained. The dynamic behaviors analysis shows that the fractional-order chaotic system represented better sensitivity of initial values and parameters. The randomness test indicates that the pseudo-random sequence generated by fractional-order memristor chaotic circuit has better randomness. Moreover, it has some advantages of image information encryption. Based on this chaotic system, a novel color image compression and encryption algorithm is proposed. The compression ratio research results show that the algorithm has stronger compression and reconstruction effects. The security performance analysis illustrates that the designed algorithm can resist various attack. Therefore, we presented image compression and encryption scheme can effectively compress and encrypt image, which provides experimental basis and theoretical guidance for safe transmission of image information. In the later work, we will propose more encryption and CS algorithms and continuously improve security.

REFERENCES

[1] C. Li, J. C. Sprott, and H. Xing, "Constructing chaotic systems with conditional symmetry," *Nonlinear Dyn.*, vol. 87, no. 2, pp. 1351–1358, 2017.

[2] C. Li, J. C. Sprott, and Y. Mei, "An infinite 2-D lattice of strange attractors," *Nonlinear Dyn.*, vol. 89, no. 4, pp. 2629–2639, 2017.

[3] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Process.*, vol. 143, pp. 122–133, Feb. 2018.

[4] C. K. Huang and H.-H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," *Opt. Commun.*, vol. 282, pp. 2123–2127, Jun. 2009.

[5] H. Liu, X. Wang, and A. Kadir, "Color image encryption using choquet fuzzy integral and hyper chaotic system," *Optik-Int. J. Light Electron Opt.*, vol. 124, no. 18, pp. 3527–3533, Sep. 2013.

[6] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *J. Syst. Softw.*, vol. 124, no. 23, pp. 290–299, Feb. 2012.

[7] A. Kadir, A. Hamdulla, and W.-Q. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Opt.-Int. J. Light Electron Opt.*, vol. 125, no. 5, pp. 1671–1675, Mar. 2014.

[8] R. Rhouma, S. Meherzi, and S. Belghith, "OCML-based colour image encryption," *Chaos Solitons Fractals*, vol. 40, no. 1, pp. 309–318, Apr. 2009.

[9] X. Wu, D. Wang, J. Kurths, and H. Kan, "A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system," *Inf. Sci.*, vols. 349–350, pp. 137–153, Jul. 2016.

[10] L. Xu, X. Gou, Z. Li, and J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion," *Opt. Lasers Eng.*, vol. 91, pp. 41–52, Apr. 2017.

[11] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, vol. 90, pp. 238–246, Mar. 2017.

[12] S. M. Ismail *et al.*, "Biomedical image encryption based on double-humped and fractional logistic maps," in *Proc. 6th Int. Conf. Mod. Circuits Syst. Technol. (MOCAST)*, May 2017, pp. 1–4.

[13] J.-F. Zhao, S.-Y. Wang, L.-T. Zhang, and X.-Y. Wang, "Image encryption algorithm based on a novel improper fractional-order attractor and a wavelet function map," *J. Elect. Comput. Eng.*, vol. 2017, Mar. 2017, Art. no. 8672716.

[14] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," *Nonlinear Dyn.*, vol. 78, no. 2, pp. 995–1015, Oct. 2014.

[15] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, "A novel color image encryption algorithm based on spatial permutation and quantum chaotic map," *Nonlinear Dyn.*, vol. 8, nos. 1–2, pp. 511–529, Jul. 2015.

[16] X. Wang and H.-L. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dyn.*, vol. 83, nos. 1–2, pp. 333–346, 2016.

[17] X. Wu, K. Wang, X. Wang, and H. Kan, "Lossless chaotic color image cryptosystem based on DNA encryption and entropy," *Nonlinear Dyn.*, vol. 90, no. 2, pp. 855–875, Oct. 2017.

[18] M. L. Sahari and I. Boukemara, "A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption," *Nonlinear Dyn.*, vol. 94, no. 1, pp. 723–744, Oct. 2018.

[19] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.

[20] Z. Gan, X. Chai, M. Zhang, and Y. Lu, "A double color image encryption scheme based on three-dimensional Brownian motion," *Multimedia Tools Appl.*, vol. 77, pp. 27919–27953, Nov. 2018.

[21] X. Chai, Z. H. Gan, L. Yang, M.-H. Zhang, and Y.-R. Chen, "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system," *Chin. Phys. B*, vol. 25, no. 10, pp. 76–88, Aug. 2016.

[22] X. Wu, Y. Li, and J. Kurths, "A new color image encryption scheme using CML and a fractional-order chaotic system," *PLoS ONE*, vol. 10, no. 3, 2015, Art. no. e0119660. doi: 10.1371/journal.pone.0119660.

[23] X. Wang, Q. Wang, and Y. Zhang, "A fast image algorithm based on rows and columns switch," *Nonlinear Dyn.*, vol. 79, no. 2, pp. 1141–1149, 2015.

[24] K. B. Oldham and J. Spanier, *The Fractional Calculus: Theory and Applications of Differentiation and Integration to Arbitrary Order*. New York, NY, USA: Dover, 2002.

[25] S. Bhalekar, "Dynamical analysis of fractional order Uçar prototype delayed system," *Signal Image Video Process.*, vol. 6, no. 3, pp. 513–519, 2016.

[26] S. He, K. Sun, and H. Wang, "Complexity analysis and DSP implementation of the fractional-order lorenz hyperchaotic system," *Entropy*, vol. 17, no. 12, pp. 8299–8311, Dec. 2015.

[27] L. Zhang, K. Sun, S. He, H. Wang, and Y. Xi, "Solution and dynamics of a fractional-order 5-D hyperchaotic system with four wings," *Eur. Phys. J. Plus*, vol. 132, p. 31, Jan. 2017.

[28] J. Ruan, K. Sun, J. Mou, L. Zhang, and S. He, "Fractional-order simplest memristor-based chaotic circuit with new derivative," *Eur. Phys. J. Plus*, vol. 133, p. 3, Jan. 2018.

[29] L. Chua and G. Alexander, "The effects of parasitic reactances on nonlinear networks," *IEEE Trans. Circuit Theory*, vol. 18, no. 5, pp. 520–532, Sep. 1971.

[30] H. Wu, B. Bao, Z. Liu, Q. Xu, and P. Jiang, "Chaotic and periodic bursting phenomena in a memristive Wien-bridge oscillator," *Nonlinear Dyn.*, vol. 83, nos. 1–2, pp. 893–903, Jan. 2016.

[31] Q. Yu, B. Bao, F. W. Hu, Q. Xu, M. Chen, and J. Wang, "Wien-bridge chaotic oscillator based on fisrt-order generalized memristor," *Acta Phys. Sinica*, vol. 63, no. 24, 2014, Art. no. 240505.

[32] M. Chen, M. Li, Q. Yu, B. Bao, Q. Xu, and J. Wang, "Dynamics of self-excited attractors and hidden attractors in generalized memristor-based Chua's circuit," *Nonlinear Dyn.*, vol. 81, nos. 1–2, pp. 215–226, 2015.

[33] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, "The missing memristor found," *Nature*, vol. 453, pp. 80–83, May 2008.

[34] X. Ye, J. Mou, C. Luo, and Z. Wang, "Dynamics analysis of Wien-bridge hyperchaotic memristive circuit system," *Nonlinear Dyn.*, vol. 92, no. 3, pp. 923–933, May 2018.

[35] Q. Tan, Y. Zeng, and Z. Li, "A simple inductor-free memristive circuit with three line equilibria," *Nonlinear Dyn.*, vol. 94, no. 3, pp. 1585–1602, Nov. 2018.

[36] J. Sun, X. Zhao, J. Fang, and Y. Wang, "Autonomous memristor chaotic systems of infinite chaotic attractors and circuitry realization," *Nonlinear Dyn.*, vol. 94, no. 4, pp. 2879–2887, 2018.

[37] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[38] X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, "A joint color image encryption and compression scheme based on hyper-chaotic system," *Nonlinear Dyn.*, vol. 84, no. 4, pp. 2333–2356, 2016.

[39] H. Zhu, C. Zhao, and X. Zhang, "A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem," *Signal Process. Image Commun.*, vol. 28, no. 6, pp. 670–680, Jul. 2013.

[40] D. Zhang, X. Liao, B. Yang, and Y. Zhang, "A fast and efficient approach to color-image encryption based on compressive sensing and fractional Fourier transform," *Multimedia Tools Appl.*, vol. 77, no. 2, pp. 2191–2208, Jan. 2018.

[41] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Process*, vol. 134, pp. 35–51, May 2017.

[42] E. J. Candès, "The restricted isometry property and its implications for compressed sensing," *Comp. Rendus Math.*, vol. 346, nos. 9–10, pp. 589–592, May 2008.

[43] H. Bao, T. Jiang, K. Chu, M. Chen, Q. Xu, and B. Bao, "Memristor-based canonical Chua's circuit: Extreme multistability in voltage-current domain and its controllability in flux-charge domain," *Complexity*, vol. 2018, Mar. 2018, Art. no. 5935637.

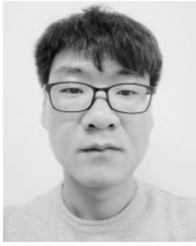
[44] A. L. Rukhin, J. Soto, and J. R. Nechvatal, "SP 800-22 Rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications," *Appl. Phys. Lett.*, vol. 22, no. 7, pp. 179–1645, 2010.

[45] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Process.*, vol. 148, pp. 124–144, Jul. 2018.

[46] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Process., Image Commun.*, vol. 52, pp. 6–19, Mar. 2017.

[47] W. Liu, K. Sun, Y. He, and Y. Yu, "Color image encryption using three-dimensional sine ICMIC modulation map and DNA sequence operations," *Int. J. Bifurcation Chaos*, vol. 27, no. 11, 2017, Art. no. 1750171.

[48] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.



FEIFEI YANG received the B.E. degree from Longdong University, Qingyang, China, in 2016. He is currently pursuing the Ph.D. degree in control science and engineering with the Dalian Polytechnic University, Dalian, China. His current research interest includes chaos theory and application.

JUN MOU received the B.S., M.S., and Ph.D. degrees in physics and electronics from Central South University, Changsha, China. He is currently an Associate Professor with the School of Information Science and Engineering, Dalian Polytechnic University, China. His current research interests include nonlinear system control, secure communication, power system automation, and smart grid research.

KEHUI SUN received the B.S. degree in industrial automation and the Ph.D. degree in control theory and control engineering from Central South University, Changsha, China, in 1998 and 2005, respectively, where he is currently a Professor with the School of Physics and Electronics. His current research interests include the chaos synchronization control theory and its application in secure communication, and intelligent instrument development.

YINGHONG CAO received the B.S. degree in electronic engineering and the Ph.D. degree in signal and information processing from the Dalian University of Technology (DUT), Dalian, China, in 2003 and 2013, respectively. She is currently a Lecturer with the School of Information Science and Engineering, Dalian Polytechnic University. Her research interests include communication signal processing, speech processing, and the Internet of Things technology and application.

JIYU JIN received the Ph.D. degree in information and communication engineering from Yeungnam University, Gyeongsan, South Korea, in 2007. He is currently an Associate Professor with the School of Information Science and Engineering, Dalian Polytechnic University, China. His research interests include wireless/mobile communication systems and the Internet of Things.